CLAIMS

1. An apparatus (N-41, N-42) arranged for receiving a Single Sign-On service request in a telecommunication service network (N-40) from a user (N-10) via an access network (N-20) unable to provide data origin authentication, the user (N-10) having received (S-23) access credentials (Digital Certificate) as a result of being authenticated by a core network (N-30), the apparatus comprising:

- means for receiving (S-24) the access credentials from the user (N-10) through the access network (N-20);
- means for checking (N-41; S-25, N-31) validity of the access credentials received from the user (N-10);
- means for establishing a valid session with the user (N-10) upon successful validity check of the access credentials;
- means for assigning an internal IP address to identify the user in the service network (N-40); and
- means for linking (N-41, S-26, N-42) session data, access credentials and assigned internal IP address for the user (N-10);

and **characterised in that** it includes:

- means for establishing a secure tunnel (S-24) with the user (N-10) when receiving the access credentials through the access network (N-20) by using an outer IP address assigned to the user by the access network for addressing the user, and by using the internal IP address assigned to identify the user in the service network (N-40) as an inner IP address in the tunnelled traffic.

2. The apparatus of claim 1, further comprising means for generating service credentials (N-41, S-26, N-42) for authorizing the user to access a service in the service network (N-40).

3. The apparatus of claim 2, wherein the service credentials are generated (N-41, S-26, N-42) on a per service basis for the user upon service request.

4. The apparatus of claim 1, further comprising means for communicating (S-25) with an Authentication Server (N-31) of the home network (N-30) in order to check the validity of the access credentials received from the user (N-10), when said access credentials are not signed by a recognised authentication entity (N-31).

5. The apparatus of claim 1, wherein the means for establishing the secure tunnel (S-24) with the user (N-10) are included in a first device named Secure Service Entry Point (N-41), and the means for linking session data, access credentials and assigned internal IP address for the user (N-10) are included in a second device named Single Sign-On server (N-42).

6. The apparatus of claim 5, further comprising means for communicating (S-26) the Secure Service Entry Point (N-41) with the Single Sign On Server (N-42).

7. The apparatus of claim 1, further comprising means for an additional co-ordination (S-25) between the apparatus (N-41; N-42) and an Identity Provider (N-31) in charge of said user in a home network (N-30) when said home network is different than the service network (N-40) which the apparatus is the entry point for.

8. The apparatus of claim 1 for use when the user (N-10) is accessing a local HTTP service (N-44), or an external service (N-51) in a network (N-50) different than the currently accessed service network (N-40), the apparatus having means for checking (N-41, S-30, N-43, S-28, N-42) whether the user had been previously authenticated or not.

9. The apparatus of claim 8, having means (S-30, S-28) for communicating with an intermediate entity (N-43) arranged to

intercept the user's access (S-29) to the HTTP local service (N-44), or to the external service (N-51) in an external network (N-50).

10. The apparatus of claim 9, wherein the intermediate entity (N-43) is an HTTP-proxy.

11. The apparatus of claim 9, wherein the intermediate entity (N-43) is a firewall.

12. The apparatus of claim 1 for use when the user (N-10) is accessing a non-HTTP local service (N-45), having means for checking (N-41, S-31, N-45, S-32, N-42) whether the user had been previously authenticated or not.

13. The apparatus of claim 1, wherein the means for receiving access credentials comprises means for checking whether a digital certificate issued by the core network is present to indicate a successful authentication of the user.

14. A user equipment (N-10; N-11) arranged to carry out an authentication procedure with a core network (N-30), and arranged to access a telecommunication service network (N-40) via an access network (N-20) unable to provide data origin authentication, the user equipment (N-10; N-11) comprising:

- means for obtaining (S-23) access credentials as a result of being authenticated by the core network (N-30);
- means for sending (S-24) the access credentials towards the service network (N-40) when accessing through the access network (N-20)

and **characterised in that** it includes:

- means for establishing a secure tunnel (S-24) with the service network (N-40) through the access network (N-20), the secure tunnel making use of an

outer IP address assigned to the user by the access network for addressing the user;

- means for receiving (S-24) an internal IP address assigned by the service network (N-40) and included as an inner IP address within the tunnelled traffic to identify the user in the service network; and
- means for linking said access credentials with the inner IP address and with the secure tunnel.

15. The user equipment (N-10; N-11) of claim 14, wherein the means for obtaining access credentials includes:

- means for receiving an authentication challenge from the core network;
- means for generating and returning an authentication response to the core network;
- means for generating a public and private key pair; and
- means for submitting the public key along with a digital signature proving the ownership of the private key towards the core network.

16. The user equipment (N-10; N-11) of claim 14, wherein the means for obtaining access credentials includes:

- means for receiving an authentication challenge from the core network;
- means for generating and returning an authentication response to the core network; and
- means for requesting a digital certificate obtainable from the core network.

17. The user equipment (N-10; N-11) of claim 16, wherein the means for obtaining access credentials further includes means for

generating a public key for which the digital certificate is obtainable.

18. A method for supporting Single Sign-On services in a telecommunication service network (N-40) for a user (N-10) accessing said service network (N-40) through an access network (N-20) unable to provide data origin authentication, the user (N-10) having received (S-23) access credentials as a result of being authenticated by a core network (N-30), the method comprising the steps of:

- receiving (S-24) at the service network (N-40) the access credentials from the user (N-10) through the access network (N-20);
- checking (N-41, S-25, N-31) validity of the access credentials received at the service network (N-40);
- establishing (N-41, S-26, N-42) a valid session with the user (N-10) upon successful validity check of the access credentials;
- assigning at the service network (N-41, S-26, N-42) an internal IP address for the user (N-10) to identify the user when accessing a service in the service network; and
- linking (N-41, S-26, N-42) session data, access credentials and the assigned internal IP address for the user (N-10) at an entity (N-41; N-42) of the service network (N-40);

and **characterised by** including the steps of:

- establishing a secure tunnel (S-24) between the user equipment side (N-10) and an entity (N-41) of the service network (N-40) through the access network (N-20) by using an outer IP address assigned by the access network for addressing the user, and by using as an inner IP address in the tunnelled traffic the internal IP address assigned to identify the user in the service network (N-40); and

- linking said access credentials with said inner IP address and with said secure tunnel at the user equipment side (N-10).

19. The method of claim 18, further comprising a step of generating service credentials (N-41, S-26, N-42) for authorizing the user to access a service in the service network (N-40).

20. The method of claim 19, wherein the step of generating service credentials includes a step of generating service credentials on a per service basis for the user upon service request.

21. The method of claim 18, wherein the step of checking (N-41; N-41, S-25, N-31) the validity of access credentials received from the user (N-10) at the service network (N-40) further includes a step of communicating (S-25) with an Authentication Server (N-31) of the home network (N-30), when said access credentials are not signed by a recognised authentication entity.

22. The method of claim 18, wherein the step of linking session data, access credentials and assigned internal IP address for the user (N-10) further includes a step of communicating (S-26) a first device named Secure Service Entry Point (N-41), in charge of the secure tunnel (S-24), with a second device named Single Sign On Server (N-42) where the step of linking takes places.

23. The method of claim 18, for use when the user (N-10) is accessing a local service (N-44; N-45), or an external service (N-51) in a network (N-50) different than the currently accessed service network (N-40), the method further comprising a step of checking (S-28, N-42; S-32, N-42) whether the user had been previously authenticated or not.